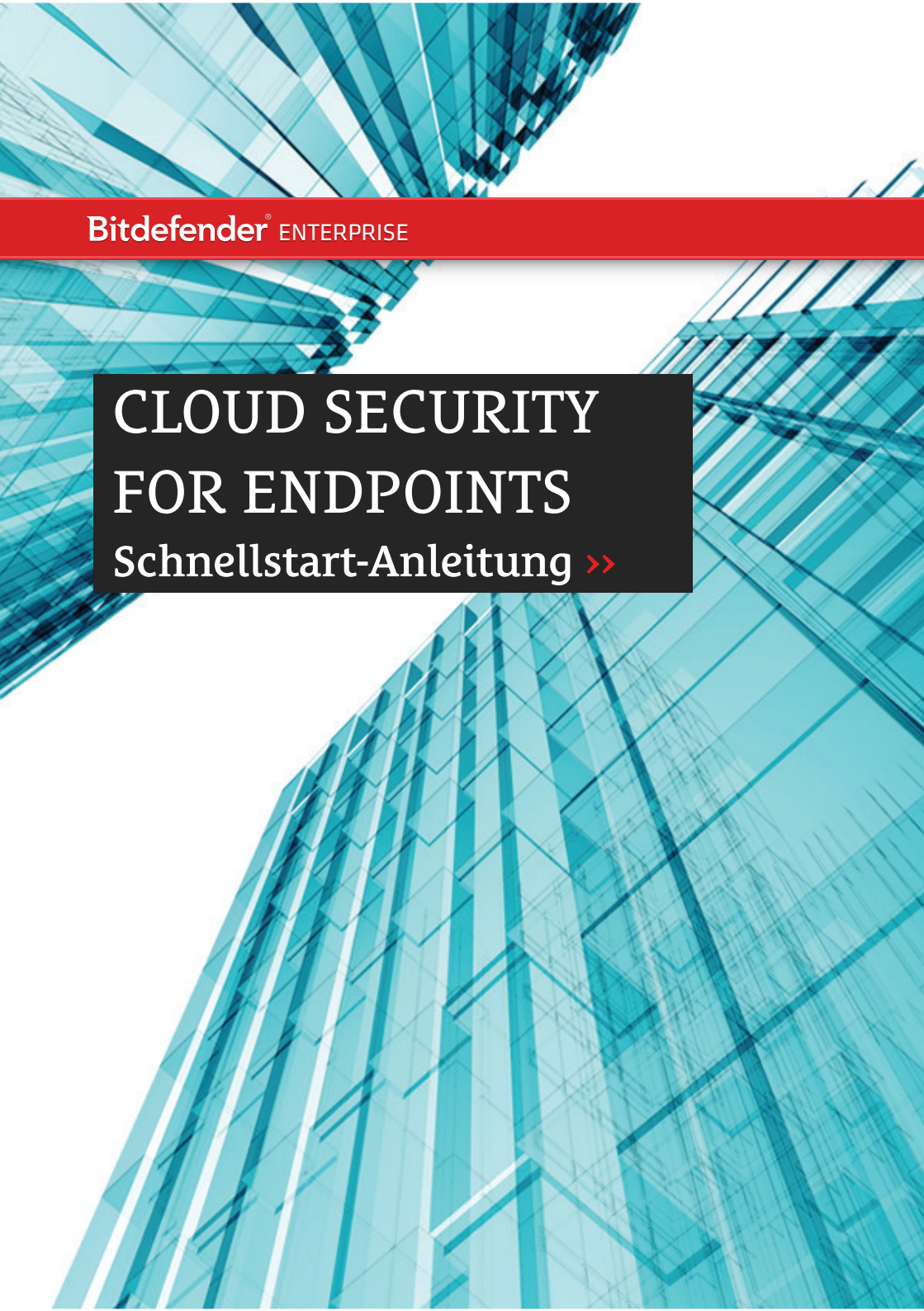

Bitdefender ENTERPRISE
CLOUD SECURITY
FOR ENDPOINTS
Schnellstart-Anleitung ››

Cloud Security for Endpoints by Bitdefender Schnellstart-Anleitung

Veröffentlicht 2013.07.31

Copyright© 2013 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation sind urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „ohne Mängelgewähr" gegeben. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokumente entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von Bitdefender erstellte Webseiten, die auch nicht von Bitdefender kontrolliert werden, somit übernimmt Bitdefender auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch der in diesem Dokument aufgelisteten Drittanbieter-Webseiten erfolgt damit auf eigene Gefahr. Bitdefender stellt diese Links der Einfachheit zur Verfügung. Dies bedeutet nicht, dass Bitdefender den Inhalt einer Website Dritter befürwortet oder Verantwortung dafür übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Bitdefender

Inhaltsverzeichnis

Zur Verwendung dieses Handbuchs ..... **v**

1. Über Cloud Security for Endpoints **1**
1.1. Architektur 2
1.2. Benutzerkonten 3
1.3. Bedrohungsschutz 4
1.3.1. Malware-Schutz 4
1.3.2. Phishing-Schutz 6
1.3.3. Firewall und Angriffserkennung 7
1.3.4. Datenschutz 7
1.3.5. Inhaltssteuerung 8
1.4. Workflow 8
1.4.1. Bereitstellung 8
1.4.2. Endpunktverwaltung 9
1.4.3. Sicherheitsrichtlinien 9
1.4.4. Scan-Aufgaben 9
1.4.5. Berichte 9

2. Erste Schritte **11**
2.1. Verbinden mit der Cloud Security Console 11
2.2. Übersicht über die Cloud Security Console 11
2.3. Verwalten Ihres Kontos 12
2.4. Ändern des Standardpassworts 14

3. Dienstleistungsabonnement **15**
3.1. Aktivieren einer Lizenz 15
3.2. Lizenzverlängerung 16
3.3. Aufstocken der Anzahl von lizenzierten Endpunkten 16
3.4. Überprüfen Ihres Abonnementstatus 16

4. Installation und Einrichtung **17**
4.1. Schritt 1 - Installation vorbereiten 17
4.2. Schritt 2 - Den Dienst auf den Computern installieren 18
4.3. Schritt 3 - Computer aufteilen (optional) 21
4.4. Schritt 4 - Eine Sicherheitsrichtlinie anlegen und konfigurieren 22

5. Überwachen des Sicherheitsstatus **25**

6. Scannen von verwalteten Computern **27**

7. Hilfe erhalten **28**

A. Anforderungen **29**
A.1. Systemanforderungen 29
A.2. Anforderungen für Netzwerkerkennung 30

Zur Verwendung dieses Handbuchs

Diese Schnellstartanleitung richtet sich an IT-Administratoren die den Cloud Security for Endpoints-Dienst nutzen möchten, um die Computer (Arbeitsplatzrechner, Laptops und Server) in ihrem Unternehmen zu schützen und zu steuern. Sie erhalten grundlegende Informationen, um sich mit dem Dienst vertraut zu machen und um ihn einzurichten und zu verwalten.

Dieses Handbuch soll neue Anwender bei der reibungslosen Einrichtung von Cloud Security for Endpoints auf den Computern im Unternehmen unterstützen.

Die hier bereitgestellten Informationen sollten für jeden Benutzer mit Erfahrung im Umgang mit Windows verständlich sein.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

Über dieses Handbuch

Dieses Handbuch ist übersichtlich gestaltet, damit Sie im Handumdrehen alle benötigten Informationen finden können.

„Über Cloud Security for Endpoints“ (S. 1)
Erfahren Sie mehr über Cloud Security for Endpoints.

„Erste Schritte“ (S. 11)
Erste Schritte mit der Cloud Security Console (der Service-Management-Konsole).

„Dienstleistungsabonnement“ (S. 15)
Hier erhalten Sie alle notwendigen Informationen über das Dienstleistungsabonnement.

„Installation und Einrichtung“ (S. 17)
Zeigt die Schritte zur Einrichtung des Dienstes auf den Computern.

„Überwachen des Sicherheitsstatus“ (S. 25)
Erfahren Sie alles über die Überwachung des Sicherheitsstatus im Netzwerk.

„Scannen von verwalteten Computern“ (S. 27)
Erfahren Sie alles über das Scannen von verwalteten Computern, um Viren und Malware zu finden.

„Hilfe erhalten“ (S. 28)
Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

„Anforderungen“ (S. 29)
Systemanforderungen für die Nutzung des Dienstes.

Zusätzliche Dokumentation

Im Folgenden erhalten Sie eine Übersicht über weitere Handbücher und Hilfetexte für Cloud Security for Endpoints:

Hilfe
Ausführliche Erläuterungen direkt in der Cloud Security Console (klicken Sie in der oberen rechten Bildschirmecke auf **Hilfe und Support**).

Administratorhandbuch
Ausführliche Dokumentation für Dienstadministratoren im PDF-Format.

Berichterstatterhandbuch
Ausführliche Dokumentation für Cloud Security Console-Anwender mit Berichterstatterrolle im PDF-Format.

Endpoint Security-Benutzerhandbuch
Ausführliche Dokumentation für Endanwender der geschützten Computer im PDF-Format.

Alle PDF-Handbücher sind im Online-Support-Center von Bitdefender verfügbar.Im Support-Center finden Sie darüber hinaus nützliche Artikel aus der Wissensdatenbank.

Konventionen in diesem Handbuch

Um die Lesbarkeit zu fördern werden verschiedene Arten von Textstilen verwendet. Die jeweiligen Bedeutungen entnehmen Sie bitte der nachfolgenden Tabelle.

Erscheinungsbild	Beschreibung
https://cloud.bitdefender.net	Verweise (Links) auf externe Inhalte wie z.B. Web-Seiten oder FTP-Server.
„Zur Verwendung dieses Handbuchs“ (S. v)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
Option	Alle Optionen in der Benutzeroberfläche werden **fett gedruckt** dargestellt.
Stichwort	Wichtige Stichwörter oder Begriffe werden durch **Fettdruck** hervorgehoben.
`Syntaxbeispiele`	Syntaxbeispiele werden in einer Schriftart mit `fester Laufweite` angegeben.

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.

Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

Warnung

Diese kritische Information sollten Sie mit höchster Aufmerksamkeit verfolgen. Hier angegebenen Anweisungen und Informationen sollten Sie auf jeden Fall Beachtung schenken. Sie sollten diese Informationen sorgsam lesen und verstanden haben, da es sich um eine höchst prekäre Thematik handelt.

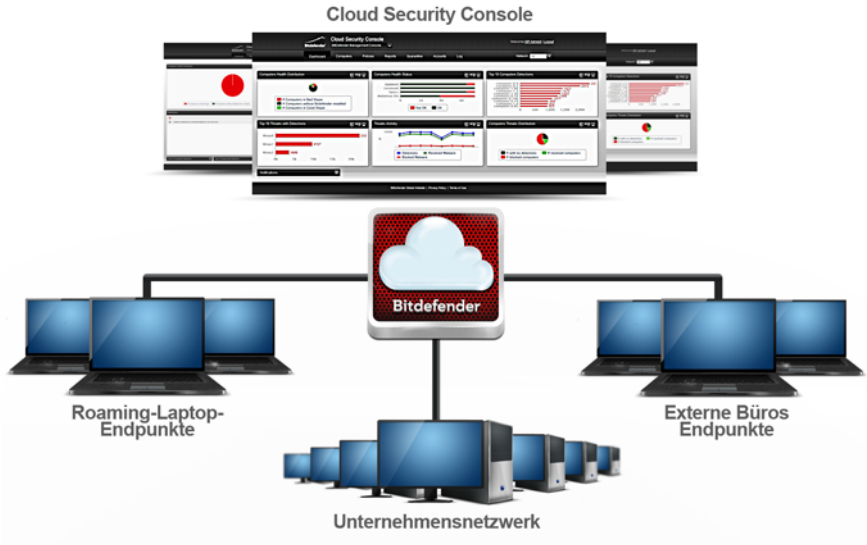
1. Über Cloud Security for Endpoints

Cloud Security for Endpoints ist ein Cloud-basierter Dienst zum Schutz vor Malware, der von Bitdefender für Computer mit dem Microsoft Windows-Betriebssystem entwickelt wurde. Der Dienst nutzt ein zentrales Software-as-a-Service-Model mit verschiedenen Bereitstellungsoptionen, die sich besonders für Unternehmenskunden eignen. Gleichzeitig kommen bewährte Malware-Schutz-Technologien zum Einsatz, die von Bitdefender für den Privatanwendermarkt entwickelt wurden.

In diesem Kapitel erhalten Sie einen ersten Überblick über Cloud Security for Endpoints:

- „Architektur“ (S. 2)
- „Benutzerkonten“ (S. 3)
- „Bedrohungsschutz“ (S. 4)
- „Workflow“ (S. 8)

1.1. Architektur



Cloud Security for Endpoints-Architektur

Die Sicherheitsdienste werden in der öffentlichen Cloud von Bitdefender gehostet. Abonnenten erhalten Zugriff auf eine Web-basierte Verwaltungsoberfläche, die sogenannte **Cloud Security Console**. Über diese Oberfläche können Administratoren per Fernzugriff den Malware-Schutz auf allen Windows-basierten Computern installieren und verwalten. Dazu gehören: Server und Arbeitsplatzrechner im internen Netzwerk, Laptop-Endpunkte im Roaming oder Endpunkte in Zweigniederlassungen.

Eine lokale Anwendung mit dem Namen **Endpoint Security** wird auf jedem geschützten Rechner installiert. Lokale Anwender haben nur begrenzten Einblick in die Sicherheitseinstellungen und können sie selbst nicht verändern. Die Einstellungen werden vom Administrator zentral über die Cloud Security Console verwaltet; Scans, Updates und Konfigurationsänderungen werden in der Regel im Hintergrund durchgeführt.

Optional ist auch ein lokaler **Update-Server** verfügbar. Der Update-Server zentralisiert die Aktualisierung und Verteilung der Endpunkt-Clients im lokalen Netzwerk und reduziert so den Internet-Datenverkehr für Netzwerke mit einer Vielzahl von Endpunkten. Mit dem Update-Server können zudem Endpoint Security-Updates auch auf Computern im Netzwerk bereitgestellt werden, die nicht mit dem Internet verbunden sind.

1.2. Benutzerkonten

Cloud Security for Endpoints setzt auf eine integrierte Umgebung zur Verteilung und Bereitstellung, in der verschiedene Kontotypen in einer hierarchischen Struktur verbunden sind. Jedes Konto ermöglicht vollen Einblick in die untergeordneten Konten. Um Nachvollziehbarkeit zu gewährleisten, werden die Aktionen der Anwender sowohl für das vorliegende Konto als auch für die untergeordneten Konten in einem Aktivitätsprotokoll festgehalten.

Es gibt vier verschiedene Kontotypen:

1. **Partner** - Cloud Security for Endpoints-Händler und -Wiederverkäufer nutzen Partnerkonten. Partnerkonten können zwei Typen von untergeordneten Konten haben: andere Partnerkonten oder Kundenkonten. Partner, die ihren Vertrieb ausbauen, können untergeordnete Partnerkonten anlegen. Beim direkten Verkauf an den Endkunden können sie Unternehmenskonten anlegen. Da Partner häufig auch als Sicherheitsdienstleister auftreten, haben sie Administratorrechte für ihre untergeordneten Unternehmenskonten.
2. **Unternehmen** - Unternehmenskonten werden Endkunden zugewiesen, die eine Cloud Security for Endpoints-Lizenz von einem Partner erwerben. Eine Kunde hat immer nur ein einziges Unternehmenskonto. Ein Unternehmenskonto ist das Hauptkonto für alle Cloud Security for Endpoints-Installationen des Kunden und ermöglicht so die zentrale Steuerung aller Sicherheitseinstellungen (es sei denn, sie werden im Falle der Zusammenarbeit mit einem Sicherheitsdienstleister von dem übergeordneten Partnerkonto überschrieben). Über das Unternehmenskonto können Betriebsaufgaben an untergeordnete Administrator- oder Berichterstatterkonten weitergegeben werden.
3. **Administrator** - Administratorkonten sind interne Konten mit Administratorrechten entweder über alle Cloud Security for Endpoints-Installationen im Unternehmen oder über eine bestimmte Computer-Gruppe. Administratoren sind zuständig für die aktive Verwaltung der Cloud Security for Endpoints-Sicherheitseinstellungen. Weitere Informationen über typische Aufgaben von Administratoren finden Sie im Kapitel „Workflow“ (S. 8).
4. **Berichterstatter** - Berichterstatterkonten sind interne Konten, die ausschließlich über Lesezugriff verfügen. Über sie erhält man nur Zugriff auf Berichte und Protokolle. Diese Berichte können Mitarbeitern bereitgestellt werden, die Überwachungsaufgaben wahrnehmen oder über die Sicherheitslage auf dem Laufenden gehalten werden müssen.

Die nachfolgende Tabelle gibt einen Überblick über die Zusammenhänge zwischen den Kontotypen:

Benutzerkonto	Kontobenutzer	Zugelassene untergeordnete Konten
Partner	Wiederverkäufer, Händler	Partner, Unternehmen
Firma	Endkunden/IT-Manager	Administrator, Berichterstatter

Benutzerkonto	Kontobenutzer	Zugelassene untergeordnete Konten
Administrator	IT-Manager, Netzwerkadministratoren	Administrator, Berichterstatter
Berichterstatter	Manager, IT-Mitarbeiter, usw.	-

1.3. Bedrohungsschutz

Cloud Security for Endpoints bietet Schutz vor einer Vielzahl von Bedrohungen. Dabei kommen die folgenden Module zum Einsatz:

- Malware-Schutz mit Signatur-Scans, heuristischen Analysen (B-HAVE) und hoch entwickelten verhaltensbasierten Heuristiken (Active Virus Control) zum Schutz vor Viren, Würmern, Trojanern, Spyware, Adware, Keyloggern, Rootkits und andere Arten von Schad-Software.
- Phishing-Schutz, Browser-Symbolleiste und Suchberater zum Schutz vor gefälschten Webseiten/Spoofing und Internet-Betrug
- Firewall und Angrifferkennungssystem zum Schutz vor Netzwerkangriffen
- Datenschutz, um Social-Engineering-Versuche und versehentliche Datenweitergabe zu verhindern
- Inhaltssteuerung zum Schutz vor Verstößen gegen Unternehmensrichtlinien durch Internet-Zugriff und Anwendungsnutzung

1.3.1. Malware-Schutz

Bitdefenders Technologie zur Erkennung von Malware basiert auf 3 Schutzebenen:

1. Zunächst kommt eine herkömmliche Scan-Methode zum Einsatz, bei der die überprüften Inhalte mit der **Signaturdatenbank** abgeglichen werden. Die Signaturdatenbank enthält die Byte-Folgen, die für bekannte Bedrohungen spezifisch sind, und wird von Bitdefender regelmäßig aktualisiert. Diese Scan-Methode erkennt bestätigte Bedrohung, die bereits erforscht und dokumentiert wurden, sehr effektiv. Doch auch wenn die Signaturdatenbank immer umgehend aktualisiert wird, gibt es zwischen der Entdeckung der Bedrohung und der Problemlösung immer ein Zeitfenster, in dem das System eine Schwachstelle hat.
2. Neue, bisher noch nicht dokumentierte Bedrohungen werden in einer zweiten Schutzebene aufgefangen. Dabei handelt es sich um **B-HAVE**, die heuristische Engine von Bitdefender. Heuristische Algorithmen erkennen Malware anhand bestimmter Verhaltensweisen. B-HAVE führt mutmaßliche Malware in einer virtuellen Umgebung aus, um die Auswirkungen auf das System zu untersuchen und eine Bedrohung auszuschließen. Sollte eine Bedrohung erkannt werden, wird eine Ausführung des Programms verhindert.
3. Für Bedrohungen, die selbst von der heuristische Engine nicht erkannt werden, wurde mit **Active Virus Control (AVC)** eine dritte Schutzebene eingerichtet. Active Virus Control

überwacht ununterbrochen die laufenden Prozesse und bewertet verdächtige Verhaltensweisen wie zum Beispiel das Verbergen des Prozesstyps, die Ausführung von Code im Adressraum eines anderen Prozesses (Übernahme des Prozessspeichers zur Erweiterung von Rechten), Replikationsversuche, das Ablegen von Dateien, das Verbergen vor Anwendungen zur Prozessübersicht usw. Mit jedem verdächtigen Verhalten werden neue Punkte für den Prozess vergeben. Sobald ein Schwellenwert überschritten wird, wird ein Alarm ausgelöst.

Cloud Security for Endpoints bietet Schutz vor einer Vielzahl von Malware-Typen, so zum Beispiel:

- **Viren** - Ein Computer-Virus ist ein Computer-Programm, das sich nach Ausführung selbst repliziert und dabei häufig in scheinbar harmlose ausführbare Dateien, Startdatensätzen, Skriptdateien, Makros usw. eingebettet ist. Viren können sich nicht nur selbst replizieren, sondern enthalten meist auch eine Schadensroutine, mit der sie auf dem befallenen System schädliche Aktionen ausführen können, so zum Beispiel das Löschen oder Beschädigen von Daten, das Anzeigen von beleidigenden oder störenden Nachrichten, das Beeinflussen von Anwendungen, die Installation von Trojanern oder Spyware usw.
- **Würmer** - Auch Computer-Würmer sind sich selbst replizierende Computer-Programme, die Schadensroutinen verbreiten. Im Unterschied zu Viren sind sie eigenständige Computer-Programme und können sich automatisch verbreiten, in aller Regel über das Netzwerk.
- **Trojaner** - Trojaner sind, wie der Name schon vermuten lässt, Computer-Programme, die das befallene System für Angriffe von außen verwundbar machen. Typische Schadensroutinen sind das Öffnen von Hintertüren (Methoden zum Umgehen der Authentifizierung), der Diebstahl von Daten, die Übernahme des Systems zur Verbreitung von Spam oder für Denial-of-Service-Angriffe, das Ausspionieren des Anwenders usw. Im Gegensatz zu Viren und Würmern replizieren sich Trojaner nicht selbst.
- **Spyware** - Spyware sind Computer-Programme, die unbemerkt Informationen über den Anwender sammeln und diese an einen Dritten weiterleiten. Spyware ist häufig Teil einer erwünschten Software-Anwendung. So führen viele kostenlose Tools die beworbenen Funktionen aus, spionieren aber gleichzeitig auch ihre Anwender aus.
- **Adware** - Adware-Programme sind Software-Pakete, die unerwünschte Werbung einblenden, entweder als Werbefenster oder direkt in der Benutzeroberfläche verschiedener Anwendungen (meist in Browsern). Genau wie Spyware wird Adware häufig mit anderen mehr oder weniger nützlichen Software-Typen kombiniert.
- **Keylogger** - Keylogger überwachen die Tastatureingaben des Anwenders. Sie können durchaus legitime Anwendungen haben, werden aber auch häufig von Hackern eingesetzt, um an vertrauliche Informationen wie Anmeldedaten, Kreditkartennummern, Adressen usw. zu gelangen. Keylogger werden meist über Tojaner oder Viren verbreitet.
- **Rootkits** - Rootkits sind Systemtreiber, die das Verhalten des Systems beeinflussen. Genau wie Keylogger können Sie durchaus nützliche Anwendungen haben, werden häufig

aber auch für schädliche Zwecke missbraucht, so zum Beispiel für das Verbergen von Schad-Software, das Verhindern der Malware-Entfernung, die Erweiterung von Privilegien für nicht autorisierte Benutzer, das Öffnen von Hintertüren usw. Da sie die systemnahen Funktionen des Betriebssystems beeinträchtigen, können Rootkits nach der Installation meist nur sehr schwer erkannt und entfernt werden.

1.3.2. Phishing-Schutz

Das Modul für den Phishing-Schutz warnt und schützt vor gefälschten Webseiten und Internet-Betrug. Das Modul für den Phishing-Schutz besteht aus drei Komponenten:

- Der **Phishing-Schutz** blockiert automatisch bekannte Phishing-Seiten, um zu verhindern, dass Benutzer unbeabsichtigt persönliche oder vertrauliche Informationen an Online-Betrüger weitergeben. Neben gefälschten Webseiten werden auch andere Arten von Online-Bedrohungen unterdrückt, so zum Beispiel Verkaufsbetrug, "Schnelles Geld"-Betrug, Internet-Marketing-Betrug, Klick-Betrug usw. Anstelle der bösartigen Seite wird eine spezielle Warnseite im Browser angezeigt, die dem Benutzer mitteilt, dass die angeforderte Seite gefährlich ist.
- Die **Bitdefender-Symbolleiste** informiert Anwender über die Sicherheit der von ihnen besuchten Internet-Seiten. Mit einem Click auf einen kleinen Dragger oben im Browser-Fenster erfahren Anwender auf einen Blick, ob die aktuell angezeigte Seite sicher, verdächtig oder unsicher ist.
- Der **Suchberater** bewertet die Ergebnisse von Suchmaschinenanfragen sowie Facebook- und Twitter-Links und platziert ein Symbol vor jedem Ergebnis. Die Symbole zeigen an, ob der jeweilige Link auf eine sichere, verdächtige oder unsichere Seite verweist.

Durch den Phishing-Schutz von Cloud Security for Endpoints werden zwei Arten von Bedrohungen bekämpft:

- **Spoofing** - Dabei handelt es sich um gefälschte Webseiten mit schädlichen Inhalten, die seriöse Internet-Auftritte nachahmen, um in betrügerischer Absicht Besucher dazu zu bewegen, private Daten wie Anmelde- oder Kreditkarteninformationen preiszugeben.
- **Internet-Betrug** - Webseiten, die nicht anderen Seiten nachempfunden sind, sondern den Anschein eines seriösen Internet-Auftritts erwecken sollen und versuchen, Besucher mit verschiedenen Betrugsmaschen um ihr Geld zu bringen:
  - **Verkaufsbetrug** - Online-Anbieter, die die beworbenen Produkte nicht ausliefern.
  - **Finanzbetrug** - So zum Beispiel Betrugsversuche, die von angeblichen Finanzinstitutionen ausgehen.
  - **"Get-Rich-Quick"-Betrug** - Zum Beispiel Schneeballsysteme, Heimarbeit-Betrugsversuche oder andere Betrugsmaschen, die schnelles Geld versprechen.

- **Internet-Marketing-Betrug** - Schädliches Webseiten, die es auf Kreditkarteninformationen abgesehen haben und zum Beispiel eine angebliche Altersprüfung durchführen oder fragwürdige Gesundheitsprodukte verkaufen.
- **Klick-Betrug** - Webseiten, die Besucher durch Täuschung dazu verleiten, auf Links zu klicken, die auf andere als die angegebenen Ziele verweisen.
- **Sittenwidrige Verbreitung** - Domänen, die über Spam-Nachrichten, Kommentar-Spam, Klick-Betrug, betrügerische Inhalte in sozialen Netzwerken oder andere unredliche Methoden beworben wurden.

1.3.3. Firewall und Angriffserkennung

Die Firewall und das Angriffserkennungssystem (IDS) schützen das System vor Netzwerkbedrohungen:

- Die **Firewall** steuert den Zugriff von Anwendungen auf Netzwerkressourcen und -dienste sowie auf das Internet. Einer umfangreichen Sammlung von bekannten und seriösen Anwendungen kann der Zugriff automatisch ermöglicht werden. Zudem kann die Firewall das System vor Port-Scans schützen, die gemeinsame Nutzung der Internet-Verbindung (ICS) beschränken und Benachrichtigungen generieren, sobald neue Knoten mit dem Drahtlosnetzwerk verbunden werden.
- Das **Angrifferkennungssystem** schützt das System vor bestimmten Aktionen, die potenziell schädlich sein können, so zum Beispiel eine DLL-Injection, die Installation von Malware-Treibern, die Änderung von Bitdefender-Dateien durch Dritte, das Ausnutzen von Sicherheitslücken im Internet Explorer oder die Überwachung durch Keylogger.

1.3.4. Datenschutz

Das Modul für den Datenschutz verhindert, dass Anwender unwissentlich bestimmte vertrauliche Daten preisgeben, indem es den ausgehenden E-Mail-(SMTP) und Internet-(HTTP) Datenverkehr überprüft und den Versand von vordefinierten Zeichenfolgen blockiert. Diese Zeichenfolgen können sensible Daten enthalten, so zum Beispiel Kontonamen, Namen von sich in Entwicklung befindlichen Produkten oder Technologien, Kontaktdaten von Führungskräften usw. Hier sind insbesondere zwei Formen der Datenweitergabe weit verbreitet:

- **Social Engineering** - Dies bezeichnet den Versuch, eine Person innerhalb eines Unternehmens so zu manipulieren, dass diese vertrauliche Informationen preisgibt. Dabei gibt sich der Angreifer zum Beispiel als Kollege oder Vorgesetzter aus, spiegelt falsche Tatsachen vor oder versucht das Opfer anderweitig in seinen Handlungen zu beeinflussen.
- **Versehentliche Datenweitergabe** - In diesen Fällen handelt der Anwender fahrlässig und gibt die Daten weiter, ohne dazu vom Empfänger verleitet zu werden. Auch wenn es sich hierbei nicht um einen vorsätzlichen Datendiebstahl handelt, kann dies auch schwerwiegende Folgen haben.

1.3.5. Inhaltssteuerung

Das Modul für die Inhaltssteuerung schränkt den Benutzerzugriff auf das Internet und andere Anwendungen entweder vollständig oder zeitgesteuert ein. Die Beschränkung des Internet-Zugriffs kann auch für bestimmte Adressen, HTTP- oder SMTP-Verkehr mit festgelegten Schlüsselwörtern oder vordefinierte Kategorien von Webseiten erfolgen. Dabei können mehr als 30 Typen von Webseiten ausgeschlossen werden, so zum Beispiel solche, die Glücksspiele und nicht jugendfreie Inhalte anbieten, soziale Netzwerke, Filesharing- und Spiele-Seiten.

Das Modul für die Inhaltssteuerung hilft bei der Durchsetzung der Unternehmensrichtlinien für den Internet-Zugriff und verhindert so Produktivitätsverluste durch untätige Mitarbeiter und reduziert die Kosten für den Datenverkehr.

1.4. Workflow

Cloud Security for Endpoints-Adminisstratoren können eine Vielzahl von Aufgaben übernehmen. Den folgenden Bereichen kommt dabei eine besondere Bedeutung zu:

- Bereitstellung
- Endpunktverwaltung
- Sicherheitsrichtlinien
- Scan-Aufgaben
- Berichte

1.4.1. Bereitstellung

Der Endpoint Security kann entweder lokal oder per Fernzugriff installiert werden:

- **Lokale Installation** - Für eine lokale Installation wird ein allgemeines oder benutzerdefiniertes Installationspaket auf dem Ziel-Computer ausgeführt. Dieses Paket kann über ein lokales Speichermedium oder ein Netzwerkspeichergerät aufgerufen oder über die Bitdefender-Cloud heruntergeladen werden. Der Administrator kann benutzerdefinierte Installationspakete mit vordefinierten Einstellungen für die installierten Module, Passwörter und Upgrade-Adressen einrichten. Die Bereitstellung kann zum Beispiel erfolgen, indem der Administrator in der Bitdefender-Cloud ein benutzerdefiniertes Installationspaket einrichtet und dem lokalen Anwender per E-Mail einen entsprechenden Download-Link sendet. Der Anwender lädt dann das Installationspaket herunter und führt es aus, ohne die Installationsparameter zu verändern.
- **Ferninstallation** - Wenn Endpoint Security auf einem Computer installiert wird, scannt das Programm selbstständig das Netzwerk und dient zudem als Bereitstellungsassistent. Erkannte Computer werden in der Cloud Security Console angezeigt, damit der

Administrator Endpoint Security per Fernzugriff auf den anderen Computern im lokalen Netzwerk bereitstellen kann.

1.4.2. Endpunktverwaltung

Endpunkte können einzeln oder zusammengefasst als Gruppen verwaltet werden. Administratoren können verschiedene Computer mit übereinstimmenden Sicherheitsanforderungen zu Gruppen zusammenfassen, um so gemeinsame Sicherheitsrichtlinien anzuwenden, Berichte zu erstellen und Scan-Aufgaben auszuführen. In großen Netzwerken können die Computer-Gruppen auch von mehreren Administratoren verwaltet werden, um die Arbeit gleichmäßig zu verteilen.

1.4.3. Sicherheitsrichtlinien

In Cloud Security for Endpoints werden die Sicherheitseinstellungen mithilfe von Sicherheitsrichtlinien immer als Paket verwaltet. Eine Sicherheitsrichtlinie ist eine Konfiguration, in der bestimmte Werte festgelegt werden für:

- die Einstellungen für die Endpunkt-Benutzeroberfläche, so zum Beispiel Sichtbarkeit, Statuswarnungen und Informationen zum technischen Support
- die allgemeinen Einstellungen, so zum Beispiel Protokollierung, Passwortschutz und Updates
- Sicherheitseinstellungen, und zwar: Malware-Schutz, Firewall und Inhaltssteuerungsmodule

Um die Einhaltung von Sicherheitsrichtlinien durchzusetzen, werden Sicherheitsrichtlinien immer als vordefinierte allumfassende Profile angewendet, die auf die jeweilige Funktion des Ziel-Computers angepasst werden. Das Anwenden von individuellen Sicherheitseinstellungen für einzelne Computer oder Computer-Gruppen ist nicht möglich.

1.4.4. Scan-Aufgaben

Administratoren können über die Cloud Security Console jederzeit manuelle Scans der verwalteten Endpunkte durchführen. Mithilfe der Sicherheitsrichtlinien können zudem regelmäßige Scan-Aufgaben konfiguriert und geplant werden, die dann automatisch auf den Ziel-Computern ausgeführt werden. Quick Scans und vollständige System-Scans können entweder manuell oder als geplante Aufgabe ausgeführt werden. Geplante Aufgaben ermöglichen auch das Festlegen von benutzerdefinierten Scans.

1.4.5. Berichte

Berichte enthalten grafische Darstellungen und Listen von Sicherheitsdaten, die aus verschiedenen Computern oder Computer-Gruppen zusammengeführt werden. Dabei werden unter anderem die folgenden Daten abgedeckt: Endpoint Security-Update-Status,

Schutzstatus, Lizenzstatus, Netzwerkaktivität, Malware-Aktivität, die Top 10 der erkannten Malware usw. Berichte können entweder manuell erstellt werden oder es kann ein Zeitplan für die automatische Erstellung regelmäßiger Berichte festgelegt werden.

2. Erste Schritte

Cloud Security for Endpoints kann mit der Cloud Security Console konfiguriert und verwaltet werden. Dabei handelt es sich um eine von Bitdefender gehostete, webbasierte Oberfläche.Der Zugriff auf die Cloud Security Console erfolgt über Benutzerkonten.

Nach Ihrer Anmeldung für die Testversion oder dem Erwerb des Dienstes erhalten Sie eine E-Mail vom Bitdefender-Registrierungsservice.Die E-Mail enthält Ihre Anmeldeinformationen.

2.1. Verbinden mit der Cloud Security Console

Der Zugriff auf die Cloud Security Console erfolgt über Benutzerkonten.Sie erhalten Ihre Anmeldeinformationen per E-Mail, sobald Ihr Konto angelegt wurde.

Um eine Verbindung mit der Cloud Security Console aufzubauen:

1. Anforderungen:
   - Internetverbindung
   - Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari oder Opera
   - Empfohlene Bildschirmauflösung: 1024x768 oder höher.
2. Öffnen Sie Ihren Internet-Browser.
3. Öffnen Sie die folgende Webseite:https://cloud.bitdefender.net
4. Geben Sie die E-Mail-Adresse und das Passwort für Ihr Konto ein.
5. Klicken Sie auf **Anmelden**.

Beachten Sie

Sollten Sie Ihr Passwort vergessen haben, verwenden Sie den Link für die Passwortwiederherstellung, um ein neues Passwort anzufordern.Sie müssen die E-Mail-Adresse Ihres Kontos angeben.

Bei der ersten Anmeldung an der Konsole werden Sie aufgefordert, die Dienstleistungsvereinbarung zu lesen und den Bedingungen zuzustimmen.Wenn Sie den Bedingungen nicht zustimmen, können Sie den Dienst nicht nutzen.

2.2. Übersicht über die Cloud Security Console

Cloud Security Console ist so aufgebaut, dass Sie schnellen Zugriff auf alle Funktionen erhalten.

Verwenden Sie die Menüleiste im oberen Bereich, um durch die Konsole zu navigieren.

Dashboard
Übersichtliche Diagramme anzeigen, die wichtige Sicherheitsinformationen über Ihr Netzwerk enthalten.

Computer
Schutz installieren, Computer verwalten und Aufgaben per Fernzugriff ausführen.

Richtlinien
Sicherheitsrichtlinien anlegen, anwenden und verwalten.

Berichte
Sicherheitsberichte über verwaltete Computer erhalten.

Quarantäne
Dateien in Quarantäne per Fernzugriff verwalten.

Konten
Ihre Kontoinformationen und -einstellungen verwalten.Benutzerkonten für andere Mitarbeiter des Unternehmens anlegen und verwalten.

Protokoll
Das Benutzeraktivitätsprotokoll einsehen.

Im oberen rechten Konsolenbereich finden Sie die folgenden Links:

- **Benutzername.** Klicken Sie auf Ihren Benutzernamen, um Ihre Kontoinformationen und -einstellungen zu bearbeiten.
- **Hilfe und Support.** Klicken Sie auf diesen Link, um Hilfe- und Support-Informationen zu erhalten.
- **Abmelden.** Klicken Sie auf diesen Link, um sich bei Ihrem Konto abzumelden.

2.3. Verwalten Ihres Kontos

Um Ihre Kontoinformationen und -einstellungen zu überprüfen und zu verändern:

1. Öffnen Sie die Seite **Konten > Mein Konto**.
2. Korrigieren oder aktualisieren Sie Ihre Kontoinformationen unter **Benutzerkontodetails**.
   - **Vollständiger Name.**
   - **E-Mail.** Dies ist Ihre E-Mail-Adresse für die Anmeldung und den Kontakt.An diese Adresse werden Berichte und wichtige Sicherheitsbenachrichtigungen geschickt.Es werden automatisch E-Mail-Benachrichtigungen versandt, sobald wichtige Risikobedingungen im Netzwerk erkannt werden.
   - **Passwort.** Um das Anmeldepasswort zu ändern, geben Sie ein neues Passwort in die entsprechenden Felder ein.
   - **Name des Unternehmens.**

3. Unter **Lizenz** können Sie die Informationen zu Ihrem Abonnement einsehen.Ihr Abonnement wird von Bitdefender oder dem Bitdefender-Partner verwaltet, der den Dienst bereitstellt.Weitere Informationen finden Sie unter „Dienstleistungsabonnement“ (S. 15).
4. **Proxyverwaltung**. Wenn das Unternehmen die Verbindung zum Internet über einen Proxy-Server herstellt, müssen Sie die Proxy-Einstellungen aktivieren und konfigurieren. Sonst können die Clients, die auf den Computern installiert sind, nicht mit dem Cloud Security Console kommunizieren.

   Beachten Sie
   Unternehmen, die Proxy-Authentifizierung verwenden, können Endpoint Security nur mit einem vollständigen Installations-Kit auf Computern installieren.

   Warnung
   Wenn der Proxy-Server des Unternehmens geändert werden soll, müssen Sie zunächst im Cloud Security Console die Proxy-Einstellungen des Unternehmens durch die neuen ersetzen, bevor Sie den Wechsel zum neuen Proxy-Server durchführen können.

5. Konfigurieren Sie die Kontoeinstellungen unter **Einstellungen** nach Ihren Wünschen.
   - **Nach Anmeldung E-Mail-Benachrichtigung versenden**. Aktivieren Sie diese Option, wenn Sie jedes Mal benachrichtigt werden möchten, wenn eine Anmeldung mit Ihren Zugangsdaten erfolgt. Die Nachricht, die an Ihre E-Mail-Adresse gesendet wird, enthält die IP-Adresse der Anfrage sowie Datum und Uhrzeit der Anmeldung.
   - **Zeitzone.** Wählen Sie im Menü die Zeitzone für das Konto.Die Konsole zeigt die aktuelle Zeit entsprechend der ausgewählten Zeitzone.
   - **Sprache.** Wählen Sie im Menü die Anzeigesprache für die Konsole aus.
   - Sie können definieren, wie verwaltete Computer dieses Unternehmenskontos im Cloud Security Console angezeigt werden, in dem Sie die entsprechende Option im Menü **Anzeigen** wählen:
     - **Computer-Name**, um Computer nach ihren lokalen Namen anzuzeigen (zum Beispiel `ComputerName`)
     - **FQDN** (Fully Qualified Domain Name), um Computer mit ihrem vollständigen Systemnamen, inklusive lokalem Namen und Domain-Namen anzuzeigen (zum Beispiel `ComputerName.Domain.com`). Mit dieser Option können Sie mehrere Computer mit demselben Namen und derselben IP-Adresse auseinanderhalten.

       Beachten Sie
       Diese Einstellung wird bei Online-Computern bei der nächsten Synchronisation mit dem Netzwerk angewendet (nach höchstens 30 Minuten). Sie können die Einstellung auch sofort anwenden, indem Sie den Online-Computern eine Aufgabe oder eine Richtlinie senden.

- **Logo.** Sie können das wolkenförmige Cloud Security Console-Logo durch Ihr Unternehmenslogo ersetzen.So können Sie das Layout der PDF-Berichte individuell anpassen.Um das Logo zu ändern, klicken Sie auf **Benutzerdefiniert** und laden Sie die Bilddatei mit dem Logo von Ihrem Computer hoch.Bitte beachten Sie die folgenden Einschränkungen:
  - Logo-Größe: 81x41 Pixel.
  - Unterstützte Dateiformate: PNG und JPG.

6. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

Wichtig

Sie können Ihr eigenes Konto nicht löschen.Wenn Sie den Cloud Security for Endpoints-Dienst nicht mehr in Anspruch nehmen und Ihr Konto löschen lassen möchten, wenden Sie sich bitte an Ihren Dienstanbieter.

2.4. Ändern des Standardpassworts

Sie sollten das Standardpasswort ändern, das Ihnen nach dem Abonnieren des Dienstes per E-Mail zugesandt wurde.Es empfiehlt sich darüber hinaus, Ihr Anmeldepasswort regelmäßig zu ändern.

Um das Anmeldepasswort zu ändern:

1. Öffnen Sie die Seite **Konten > Mein Konto**.
2. Geben Sie in die entsprechenden Felder ein neues Passwort ein (unter **Benutzerkontodetails**).
3. Klicken Sie auf **Senden**, um die Änderungen zu speichern.

3. Dienstleistungsabonnement

Sie können Cloud Security for Endpoints 30 Tage lang kostenlos testen.Während der Testphase stehen alle Funktionen uneingeschränkt zur Verfügung. Sie können den Dienst auf beliebig vielen Computern nutzen.Falls Sie den Dienst weiterhin nutzen möchten, müssen Sie vor Ablauf der Testphase ein kostenpflichtiges Abonnement auswählen und abschließen.

Die Anmeldung für den Dienst kann auf zwei Arten erfolgen:

- Anmeldung über einen Bitdefender-Wiederverkäufer.Unsere Wiederverkäufer stellen Ihnen alle benötigten Informationen zur Verfügung und unterstützen Sie bei der Auswahl eines Abonnements, das Ihren Zwecken gerecht wird.Einige Wiederverkäufer bieten Mehrwertdienstleistungen, so zum Beispiel Premium-Support, andere wiederum umfassende Managed Services.

  So finden Sie einen Bitdefender-Wiederverkäufer in Ihrem Land:

  1. Gehen Sie zu http://www.bitdefender.de/partners.
  2. Öffnen Sie den **Partnerfinder**.
  3. Die Kontaktinformationen der Bitdefender-Partner sollten automatisch angezeigt werden. Sollte dies nicht der Fall sein, so wählen Sie Ihr Land aus, um die Informationen anzuzeigen.
  4. Falls Sie in Ihrem Land keinen Bitdefender-Händler finden, können Sie uns gerne unter vertrieb@bitdefender.de kontaktieren.Bitte schreiben Sie uns Ihre E-Mail in Englisch, damit wir Ihnen umgehend helfen können.

- Anmeldung über die Bitdefender-Website.

Ihr Abonnement wird von Bitdefender oder dem Bitdefender-Partner verwaltet, über den Sie den Dienst erworben haben. Manche Bitdefender-Partner sind Sicherheitsdienstleister. Abhängig von Ihrer Abonnementvereinbarung wird der tägliche Betrieb von Cloud Security for Endpoints entweder intern von Ihrem Unternehmen oder extern durch den Sicherheitsdienstleister übernommen.

3.1. Aktivieren einer Lizenz

Beim ersten Abschluss eines kostenpflichtigen Abonnements erhalten Sie einen Lizenzschlüssel. Durch das Aktivieren dieses Lizenzschlüssels aktivieren Sie auch Ihr Cloud Security for Endpoints-Abonnement. Neue Lizenzschlüssel werden unter Umständen auch bei einer Verlängerung des Abonnements oder einer Aufstockung der lizenzierten Endpunkte vergeben.

Warnung
Die Aktivierung einer Lizenz überträgt deren Umfang NICHT auf die aktuelle Lizenz. Die alte Lizenz wird vielmehr durch die neue überschrieben. Wenn Sie zum Beispiel eine Lizenz für 10 Endpunkte über einer bestehenden Lizenz für 100 Endpunkte aktivieren, erhalten Sie KEIN Lizenzvolumen von 110 Endpunkten. Im Gegenteil, die Anzahl der lizenzierten Endpunkte sinkt von 100 auf 10.

Der Lizenzschlüssel wird Ihnen nach Erwerb per E-Mail zugesendet. Abhängig von Ihrer Dienstleistungsvereinbarung wird Ihr Dienstleister unter Umständen den freigegebenen Lizenzschlüssel für Sie aktivieren. Alternativ können Sie Ihre Lizenz auch manuell aktivieren. Gehen Sie dazu folgendermaßen vor:

1. Melden Sie sich über Ihr Kundenkonto an der Cloud Security Console an.
2. Öffnen Sie die Seite **Konten > Mein Konto**.
3. Klicken Sie im Bereich **Lizenz** auf den Link neben den Feldern **Lizenznummer** oder **Lizenz läuft ab**. Die Seite mit den **Lizenzinformationen** wird angezeigt. Hier werden alle Informationen zur aktuellen Lizenz angezeigt (falls eine vorliegt).
4. Geben Sie im Feld **Lizenzschlüssel** Ihren Lizenzschlüssel ein.
5. Klicken Sie auf **Schlüssel ändern** und warten Sie, bis der Autorisierungsvorgang abgeschlossen ist.

3.2. Lizenzverlängerung

Um eine Lizenz zu verlängern oder eine abgelaufene Lizenz zu reaktivieren, wenden Sie sich bitte an Ihren Dienstleister.

3.3. Aufstocken der Anzahl von lizenzierten Endpunkten

Um die aktuelle Lizenz auf weitere Endpunkte zu erweitern, wenden Sie sich bitte an den Bitdefender-Kundendienst.

3.4. Überprüfen Ihres Abonnementstatus

Um Ihren Abonnementstatus zu überprüfen:

1. Melden Sie sich über Ihr Kundenkonto an der Cloud Security Console an.
2. Öffnen Sie die Seite **Konten > Mein Konto**.
3. Klicken Sie im Bereich **Lizenz** auf den Link neben den Feldern **Lizenznummer** oder **Lizenz läuft ab**. Die Seite mit den **Lizenzinformationen** wird angezeigt. Hier werden alle Informationen zur Ihrem Abonnementstatus angezeigt.

4. Installation und Einrichtung

Sobald Sie Ihre Anmeldedaten erhalten haben, können Sie sich bei der Cloud Security Console anmelden und mit der Installation des Dienstes auf den Computern beginnen.

Die Installation und Einrichtung gestalten sich relativ einfach. Im Folgenden die wichtigsten Schritte:

1. Installation vorbereiten.
2. Den Dienst auf den Computern installieren.
3. Computer in Gruppen aufteilen (optional).
4. Eine Sicherheitsrichtlinie anlegen und konfigurieren.

4.1. Schritt 1 - Installation vorbereiten

Bevor Sie mit der Installation beginnen, sollten Sie die folgenden Hinweise beachten, um einen reibungslosen Ablauf zu garantieren:

1. Stellen Sie sicher, dass die Computer die Mindestsystemanforderungen erfüllen. Bei manchen Computern kann es notwendig werden, das neueste Service Pack für das Betriebssystem zu installieren oder Speicherplatz zu schaffen.
2. Entfernen Sie alle bereits installierten Anti-Malware-, Internet-Sicherheits- und Firewall-Lösungen von Ihren Computern (eine Deaktivierung ist nicht ausreichend). Wenn Cloud Security for Endpoints gleichzeitig mit anderen Sicherheitslösungen auf einem Computer betrieben wird, kann dies die jeweilige Funktion stören und massive Probleme auf dem System verursachen.

   Viele der Sicherheitsprogramme, mit denen Cloud Security for Endpoints nicht kompatibel ist, werden beider Installation von Endpoint Security automatisch erkannt und können im Anschluss entfernt werden. Weitere Informationen und eine Übersicht über die Sicherheitslösungen, die erkannt werden, erhalten Sie in diesem Artikel in der Wissensdatenbank.

   Wichtig
   Um die Windows-Sicherheitsfunktionen (Windows Defender, Windows Firewall) müssen Sie sich nicht kümmern. Diese werden vor Beginn der Installation automatisch deaktiviert.

3. Für die Installation benötigen Sie Administratorrechte und Zugriff auf das Internet. Stellen Sie sicher, dass diese Bedingungen erfüllt sind.

4.2. Schritt 2 - Den Dienst auf den Computern installieren

Cloud Security for Endpoints wurde für Arbeitsplatzrechner, Laptops und Server mit Microsoft® Windows als Betriebssystem entwickelt. Um Ihre Computer mit Cloud Security for Endpoints zu schützen, müssen Sie Endpoint Security (die Client-Software) auf jedem Computer installieren. Endpoint Security verwaltet den Schutz auf dem lokalen Computer. Zudem kommuniziert er mit dem Cloud Security Console, um Befehle des Administrators entgegenzunehmen und die Ergebnisse seiner Aktionen zu übermitteln.

Es gibt zwei Installationsmethoden:

- **Lokale Installation**. Verwenden Sie den Installations-Link in Ihrem Cloud Security Console-Konto, um Endpoint Security herunterzuladen und lokal auf den einzelnen Computern zu installieren. Eine weitere Möglichkeit ist es, den Benutzern im Unternehmensnetzwerk E-Mail-Einladungen mit dem Installations-Link zu schicken und sie aufzufordern, den Schutz herunterzuladen und auf ihren Computern zu installieren. Die lokale Installation wird durch einen Assistenten unterstützt.
- **Remote-Installation**. Nach der Installation auf dem Computer erkennt Endpoint Security automatisch alle ungeschützten Computer im lokalen Netzwerk. Der Cloud Security for Endpoints-Schutz kann dann auf diesen Computern per Fernzugriff von der Konsole aus installiert werden. Die Remote-Installation erfolgt im Hintergrund, ohne dass der Benutzer dies bemerkt.

Endpoint Security verfügt über eine stark eingeschränkte Benutzeroberfläche. Über sie können Anwender den Sicherheitsstatus einsehen und grundlegende Sicherheitsaufgaben (Updates und Scans) ausführen, haben jedoch keinen Zugriff auf die Einstellungen.

Die Anzeigesprache der Benutzeroberfläche auf geschützten Computern wird bei der Installation in Abhängigkeit von der für Ihr Konto eingestellten Sprache festgelegt. Um eine andere Sprache für die Benutzeroberfläche auf einem bestimmten Computer festzulegen, müssen Sie die für Ihr Konto eingestellte Sprache vorübergehend ändern und dann erst mit der Installation fortfahren (entweder über den Installationslink oder per Remote-Installation).

Lokale Installation

Die lokale Installation erfordert die Ausführung einer Installationsdatei, die Sie über die Cloud Security Console auf jeden der zu schützenden Computer herunterladen können. Es gibt zwei Arten von Installationsdateien:

- **Web-Installer**. Der Web-Installer lädt zunächst das vollständige Installationspaket von den Bitdefender-Cloud-Servern herunter und beginnt dann mit der Installation. Der Installer ist ein kleines Programm und kann sowohl auf 32-Bit- als auch auf 64-Bit-Systemen ausgeführt werden (und vereinfacht so die Verteilung). Er erfordert jedoch eine aktive Internet-Verbindung.

- **Vollständiges Installationspaket**. Hierbei handelt es sich um das vollständige Installationspaket. Mit dem Paket können Sie den Schutz auf Computern ohne Internet-Zugang oder mit langsamer Internet-Verbindung installieren. Laden Sie diese Datei auf einen mit dem Internet verbundenen Computer herunter und nutzen Sie externe Speichermedien oder eine Netzwerkfreigabe für die Verteilung auf andere Computer. Bitte beachten Sie, dass zwei Versionen zur Verfügung stehen: eine für 32-Bit-System und eine für 64-Bit-Systeme. Stellen Sie sicher, dass Sie die zum jeweiligen Computer passende Version wählen.

Für die lokale Installation:

1. Bauen Sie über Ihr Konto eine Verbindung mit der Cloud Security Console auf.
2. Öffnen Sie die Seite **Computer > Installationsbereich**.
3. Bei Bedarf können Sie die Installationsoptionen durch einen Klick auf **Paket individuell anpassen** konfigurieren.
   a. Wählen Sie die Schutzmodule aus, die Sie installieren möchten. Bitte beachten Sie, dass für Server-Betriebssysteme nur der Malware-Schutz verfügbar ist.
   b. Bei Bedarf können Sie ein Passwort einrichten, um zu verhindern, dass Benutzer Ihren Schutz entfernen. Wählen Sie **Passwortschutz deinstallieren** und geben Sie das gewünschte Passwort in die entsprechenden Felder ein.
   c. Während der automatischen Installation wird der Computer nach Malware durchsucht. In einigen Fällen kann es notwendig sein, einen Neustart durchzuführen, um die Entfernung der Malware abzuschließen.

      Wählen Sie **Automatischer Neustart (falls nötig)**, um sicherzustellen, dass gefundene Malware vor der Installation vollständig entfernt wurde. Sonst könnte die Installation fehlschlagen.
   d. Falls eine lokaler Bitdefender-Update-Server im Netzwerk eingerichtet wurde, können Sie Endpoint Security so konfigurieren, dass Aktualisierungen über diesen Server und nicht über das Internet erfolgen. Ersetzen Sie im Feld **Update-Adresse** die Internet-Update-Adresse mit der Adresse des lokalen Update-Servers. Verwenden Sie dazu eine der folgenden Syntaxoptionen:
      - `update_server_ip:port`
      - `update_server_name:port`

Beachten Sie

Die hier festgelegte Update-Adresse wird nach der Installation vorübergehend genutzt. Sobald eine Richtlinie auf den Client angewendet wird, wird die Update-Adresse den Richtlinieneinstellungen entsprechend angepasst. Um sicherzustellen, das der Client sich auch weiterhin über den lokalen Update-Server aktualisiert, konfigurieren Sie die Optionen für die Update-Adresse in den Richtlinieneinstellungen.

4. Klicken Sie auf den entsprechenden Link, um die bevorzugte Installationsdatei (Web-Installer oder vollständiges Installationspaket) herunterzuladen. Diese kann dann auf den lokalen Computern zur Installation des Schutzes ausgeführt werden. Sie können die Datei auch auf externe Speichermedien kopieren und auf anderen Computern ausführen. Um den Link anzuzeigen, klicken Sie auf die **Installations-Link**-Schaltfläche und wählen Sie **Anzeigen**.
5. Eine weitere Möglichkeit ist es, den Benutzern im Unternehmensnetzwerk E-Mail-Einladungen mit dem Installations-Link zu schicken und sie aufzufordern, den Schutz herunterzuladen und auf ihren Computern zu installieren. Um den Link per E-Mail zu verschicken, klicken Sie auf die **Installations-Link**-Schaltfläche und wählen Sie **Per E-Mail senden**. Bitte beachten Sie, dass die Benutzer den Web-Installer-Link erhalten.

Remote-Installation

Um die Bereitstellung zu vereinfachen, verfügt Cloud Security for Endpoints über einen automatischen Mechanismus zur Netzwerkerkennung. Auf dieser Grundlage kann die Client-Software (Endpoint Security) per Fernzugriff von der Cloud Security Console aus auf den Endpunkten installiert werden. Erkannte Computer werden als **Nicht verwaltete Computer** auf der Seite **Computer** angezeigt.

Damit Sie die Netzwerkerkennung und Ferninstallation durchführen können, muss Endpoint Security bereits auf mindestens einem Computer im Netzwerk installiert sein. Dieser Computer wird dann eingesetzt, um das Netzwerk zu scannen und Endpoint Security auf den noch nicht geschützten Computern zu installieren. Um die Netzwerkerkennung zu funktionieren, müssen eine Reihe von Systemanforderungen erfüllt werden. Für weitere Informationen lesen Sie bitte „Anforderungen für Netzwerkerkennung“ (S. 30).

Beachten Sie

Nachdem Endpoint Security auf einem Computer installiert wurde, kann es einige Minuten dauern, bis die anderen Computer im Netzwerk in der Cloud Security Console angezeigt werden.

Beachten Sie

Für die Installation ist es erforderlich, dass auf jedem Ziel-Computer die administrative Freigabe Admin$ aktiviert ist.

Für die Remote-Installation:

1. Öffnen Sie die Seite **Computer > Computer anzeigen**.
2. Klicken Sie in das **Anzeigen**-Menü oberhalb der Tabelle (auf der linken Seite) und wählen Sie **Nicht verwaltete Computer**.
3. Markieren Sie die Kästchen für die Computer, auf denen Sie den Schutz installieren wollen.
4. Klicken Sie auf **Aufgaben** und wählen Sie **Installieren** aus dem Menü. Das Fenster für die Installationsoptionen wird angezeigt.

5. Sie können die Standardeinstellungen für die Installation nach Bedarf anpassen.
6. Die Ferninstallation wird über einen Computer durchgeführt, auf dem Cloud Security for Endpoints bereits installiert ist (Bereitstellender Computer). Wenn Sie einen bestimmten Computer für die Ferninstallation nutzen wollen, deaktivieren Sie das Kästchen **Bereitsteller automatisch erkennen**, geben Sie den Namen oder die IP-Adresse des Computers in das entsprechende Feld ein und wählen Sie den Computer aus der Liste aus.
7. Geben Sie die Administratoranmeldeinformationen an, die für die Remote-Authentifizierung auf den ausgewählten Computern benötigt wird.

   Geben Sie den Namen und das Passwort eines Administratorkontos für jeden der ausgewählten Computer ein. Wenn Computer in einer Domäne sind, reicht es aus, die Anmeldeinformationen des Domänenadministrators einzugeben. Verwenden Sie Windows-Konventionen, wenn Sie den Namen eines Domänenbenutzerkontos eingeben (z.B. `domain\user` oder `user@domain.com`).
8. Klicken Sie auf **Installieren**. Ein Bestätigungsfenster wird angezeigt.
9. Die Aufgabe können Sie unter **Computer > Aufgaben anzeigen** anzeigen und verwalten.

4.3. Schritt 3 - Computer aufteilen (optional)

Wenn Sie eine größere Anzahl Computer verwalten (zehn und mehr), empfiehlt es sich, diese in Gruppen aufzuteilen. Durch die Aufteilung Ihrer Computer in Gruppen können Sie diese effizienter verwalten. Ein großer Vorteil ist, dass Sie Gruppenrichtlinien verwenden können, um verschiedene Sicherheitsanforderungen zu erfüllen.

Die Computer-Gruppen werden unter **Computer anzeigen** im linken Bereich angezeigt. Anfangs ist nur die Stammgruppe nach Ihrem Unternehmen benannt. Alle Computer, auf denen Sie den Cloud Security for Endpoints-Schutz installiert haben sowie die Computer, die im Netzwerk erkannt wurden, werden automatisch in diese Gruppe aufgenommen. Sie können Ihre Computer ordnen, indem Sie unter der Stammgruppe weitere Gruppen anlegen und die Computer in die entsprechenden Gruppen verschieben.

Bevor Sie Gruppen anlegen, sollten Sie sich überlegen, warum Sie diese Gruppen brauchen und sie dann nach einem bestimmten System anlegen. Sie können Computer zum Beispiel anhand von einem oder einer Kombination der folgenden Kriterien in Gruppen einteilen:

- Organisationsstruktur (Vertrieb, Marketing, Qualitätssicherung, Unternehmensführung usw.).
- Sicherheitsanforderungen (Desktop-Rechner, Laptops, Server usw.).
- Standort (Hauptsitz, Niederlassungen, mobile Angestellte, Heimarbeitsplätze usw.).

Um Ihr Netzwerk in Gruppen aufzuteilen:

1. Öffnen Sie die Seite **Computer > Computer anzeigen**.

2. Klicken Sie mit der rechten Maustaste auf die Stammgruppe im Bereich links und wählen Sie **Gruppe anlegen**. Eine neue Gruppe (mit dem Namen **Neue Gruppe**) erscheint unterhalb der Ursprungsgruppe im Strukturmenü.
3. Die neu erstellte Gruppe umbenennen.
4. Wiederholen Sie die vorausgegangenen Schritte, um weitere Gruppen anzulegen.
5. Verschieben Sie Computer von der Stammgruppe in die passende Gruppe.
   a. Markieren Sie die Kästchen für die Computer, die Sie verschieben möchten.
   b. Verschieben Sie Ihre Auswahl per Drag und Drop in die gewünschte Gruppe im Bereich links.

4.4. Schritt 4 - Eine Sicherheitsrichtlinie anlegen und konfigurieren

Nach der Installation kann der Cloud Security for Endpoints-Schutz über die Cloud Security Console mit Hilfe von Sicherheitsrichtlinien konfiguriert und verwaltet werden. Eine Richtlinie legt die Sicherheitseinstellungen fest, die auf die Ziel-Computer angewendet werden sollen.

Direkt nach der Installation wird den Computern die Standardrichtlinie zugewiesen, die mit den empfohlenen Schutzeinstellungen vorkonfiguriert ist. Öffnen Sie die Seite **Richtlinien > Richtlinien anzeigen** und klicken Sie auf den Namen der Standardrichtlinie, um die Standardschutzeinstellungen anzuzeigen. Sie können die Schutzeinstellungen nach Bedarf verändern sowie zusätzliche Schutzfunktionen konfigurieren.

Wenn Sie eine größere Anzahl Computer verwalten (zehn und mehr), könnte es ratsam sein, mehrere Richtlinien anzulegen, um die verschiedenen Einstellungen den jeweiligen Sicherheitserfordernissen anzupassen. Sie können zum Beispiel unterschiedliche Richtlinien für Arbeitsplatzrechner, Laptops und Server konfigurieren.

Um eine neue Richtlinie anzulegen:

1. Öffnen Sie die Seite **Richtlinien > Neue Richtlinie**.
2. Geben Sie einen eindeutigen Namen für die Richtlinie ein. Wenn Sie einen Namen festlegen, berücksichtigen Sie den Zweck und das Ziel der Richtlinie.
3. Wählen Sie eine Richtlinienvorlage aus dem Menü. Die neue Richtlinie enthält zunächst die Einstellungen der Richtlinienvorlage.
4. Legen Sie das Richtlinienziel fest (Computer, auf denen die Richtlinie angewendet wird). Folgende Optionen sind wählbar:
   - **Gruppen**. Wählen Sie diese Option, um die Richtlinie auf Gruppen von verwalteten Computern anzuwenden. Klicken Sie auf den entsprechenden Link und wählen Sie die gewünschte Computer-Gruppe. Die Richtlinie wird automatisch auf jeden Computer

angewendet, der zu einem späteren Zeitpunkt zu einer ausgewählten Gruppe hinzugefügt wird.

- **Computer**. Wählen Sie diese Option, um die Richtlinie auf einzelne Computern anzuwenden. Klicken Sie auf den entsprechenden Link und wählen Sie die gewünschten Computer.

5. Klicken Sie auf **Senden**, um eine Richtlinie anzulegen und die Richtlinienseite aufzurufen.
6. Konfigurieren Sie dann die Richtlinieneinstellungen. In den meisten Fällen empfiehlt sich die Nutzung der Standardsicherheitseinstellungen. Dies sind einige Funktionen, die Sie eventuell konfigurieren möchten:
   - **Passwortschutz**. Um zu verhindern, dass Benutzer mit Administratorenrechten den Schutz deinstallieren, müssen Sie ein Passwort festlegen. Öffnen Sie die Seite **Allgemein > Erweitert** und legen Sie das gewünschte Passwort fest.
   - **Update-Einstellungen**. Endpoint Security wird stündlich automatisch nach Updates suchen und diese herunterladen und installieren (Standardeinstellung). Öffnen Sie die Seite **Allgemein > Update**, um das Update-Intervall zu ändern und andere Einstellungen vorzunehmen. Wenn Ihre Firma über einen Proxy-Server mit dem Internet verbunden ist, müssen Sie die Proxy-Einstellungen angeben. Falls eine lokaler Bitdefender-Update-Server im Netzwerk eingerichtet wurde, können Sie Endpoint Security so konfigurieren, dass Aktualisierungen über diesen Server und nicht über das Internet erfolgen.
   - **Zeitgesteuerte Scan-Aufgaben**. Sie können zeitgesteuerte Scan-Aufgaben anlegen und konfigurieren, die dann regelmäßig auf den Computern ausgeführt werden. Um eine neue Scan-Aufgabe anzulegen und zu konfigurieren, öffnen Sie die Seite **Malware-Schutz > Bedarf-Scan** und klicken Sie auf **Hinzufügen**.
   - **Firewall-Berechtigungen und Regeln**. Öffnen Sie die Seite **Firewall > Erweitert**, um die Firewall-Berechtigungen einzusehen und zu konfigurieren und Firewall-Regeln für Anwendungen festzulegen, die auf Netzwerk- oder Internet-Dienste zugreifen müssen.
   - **Inhaltssteuerung**. Über das Inhaltssteuerungsmodul können Sie die gewünschten Einstellungen für Inhaltsfilter und Identitätsschutz für die Benutzeraktivität (Surfen, E-Mail und Software-Anwendungen) vornehmen. Sie haben die folgenden Möglichkeiten:
     - Den Datenverkehrs-Scan Konfigurieren
     - Den Zugang zum Internet für bestimmte Benutzer oder Anwendung während bestimmter Zeiträume zulassen oder blockieren
     - Mit Internet-Kategorienfilter ganze Kategorien von Websites entweder zulassen oder blockieren
     - Datenschutzregeln anlegen, um personenbezogene oder vertrauliche Daten jeder Art zu schützen
     - Anwendungssteuerung konfigurieren, um den Benutzerzugriff auf Anwendungen auf ihren jeweiligen Computern blockieren oder einschränken

7. Klicken Sie auf **Speichern**, um die Änderungen zu speichern und die Schutzeinstellungen auf die Ziel-Computer anzuwenden. Die neue Richtlinie wird unter **Richtlinien anzeigen** angezeigt.

Richtlinien werden sofort, nachdem sie angelegt oder verändert wurden, per Push an die Ziel-Computer übertragen. Die Einstellungen sollten in weniger als einer Minute auf den Computern übernommen werden (vorausgesetzt, dass sie online sind). Wenn ein Computer offline ist, werden die Einstellungen übernommen, sobald er wieder online ist.

5. Überwachen des Sicherheitsstatus

Das Cloud Security Console-Dashboard ist das zentrale Überwachungs-Tool inCloud Security for Endpoints.Rufen Sie die **Dashboard**-Seite regelmäßig auf, um Echtzeitinformationen über den Sicherheitsstatus des Netzwerks zu erhalten.

Das Dashboard ist eine Statusseite mit 7 Portlets, die Ihnen einen schnellen Überblick über die Sicherheitslage der geschützten Endpunkte liefert (Arbeitsplatzrechner, Laptops, Server).In den Dashboard-Portlets werden verschiedenste Sicherheitsinformationen in übersichtlichen Diagrammen angezeigt. Sie erhalten einen schnellen Überblick über Bereiche, die Ihre Aufmerksamkeit erfordern.Jedes Dashboard-Portlet enthält im Hintergrund einen detaillierten Bericht, der mit einem einfachen Klick auf das Diagramm abgerufen werden kann.

Netzwerkstatus

Versorgt Sie mit detaillierten Informationen über den allgemeinen Sicherheitsstatus des Netzwerks.Computer werden nach diesen Kriterien in Gruppen aufgeteilt:

- Auf nicht verwalteten Computer wurde der Cloud Security for Endpoints-Schutz nicht installiert. Ihr Sicherheitsstatus kann nicht bestimmt werden.
- Auf Computern, die offline sind, ist der Cloud Security for Endpoints-Schutz normalerweise installiert, es hat jedoch zuletzt keine Endpoint Security-Aktivität mehr gegeben.Der Sicherheitsstatus von Computern, die offline sind, kann nicht zuverlässig beurteilt werden, da die Statusinformationen nicht aktuell sind.
- Auf geschützten Computern wurde der Cloud Security for Endpoints-Schutz installiert und keine Sicherheitsbedrohung gefunden.
- Auf Computern mit Sicherheitslücken ist der Cloud Security for Endpoints-Schutz zwar installiert, aber bestimmte Umstände verhindern, dass der Computer optimal geschützt ist.Die Berichtsdetails zeigen Ihnen die Sicherheitsaspekte, die Ihr Eingreifen erfordern.

Computer-Status

Versorgt Sie mit verschiedenen Statusinformationen über die Computer, auf denen Cloud Security for Endpoints-Schutz installiert ist.

Top 10 der meist infizierten Computer

Zeigt Ihnen Top 10 der Netzwerk-Computer mit den meisten Infektionen über einen bestimmten Zeitraum.

Top 10 der erkannten Malware

Zeigt Ihnen die 10 häufigsten Malware-Bedrohungen, die über einen bestimmten Zeitraum im Netzwerk erkannt wurden.

Malware-Aktivität

Versorgt Sie mit übergreifenden und Computer-spezifischen Informationen über die Malware-Bedrohungen, die über einen festgelegten Zeitraum im Netzwerk erkannt wurden.Sie sehen:

- Anzahl der Funde (gefundene Dateien, die mit Malware infiziert sind)
- Anzahl der beseitigten Infektionen (Dateien, die erfolgreich desinfiziert oder in den lokalen Quarantäneordner verschoben wurden)
- Anzahl der blockierten Infektionen (Dateien, die nicht desinfiziert werden konnten, auf die der Zugriff aber verweigert wurde; so z.B. eine infizierte Datei, die mit einem proprietären Archivformat gespeichert wurde)

Status Computer-Malware

Hilft Ihnen dabei herauszufinden, wie viele und welche der Computer im Netzwerk über einen bestimmten Zeitraum von Malware-Infektionen betroffen waren und wie mit der Bedrohung umgegangen wurde.Computer werden nach diesen Kriterien in Gruppen aufgeteilt:

- Computer ohne Funde (über den festgelegten Zeitraum wurde keine Malware-Bedrohung gefunden).
- Computer mit behobener Malware (alle infizierten Dateien wurden erfolgreich desinfiziert oder in den lokalen Quarantäneordner verschoben).
- Computer mit blockierter Malware (der Zugriff auf einige der infizierten Dateien wurde verweigert)

Benachrichtigungen

Dieses Portlet ist standardmäßig minimiert und informiert Sie über aktuelle Sicherheitsrisiken im Netzwerk. Benachrichtigungen werden Ihnen ebenfalls per E-Mail übermittelt.

Einige der Portlets enthalten Statusinformationen, andere zeigen die Sicherheitsereignisse im letzten Berichtszeitraum an.Sie können den Berichtszeitraum eines Portlets anzeigen und konfigurieren, indem Sie auf die Schaltfläche in der entsprechenden Titelleiste klicken.

Das Dashboard lässt sich nach individuellen Vorlieben konfigurieren.Sie können die Portlets minimieren, um den Blick freizumachen auf die Informationen, die Sie interessieren. Wenn Sie ein Portlet minimieren, wird es im Dashboard nicht mehr angezeigt. Die entsprechende Menüleiste erscheint am unteren Bildschirmrand.Die Größe der übrigen Portlets wird automatisch an den Bildschirm angepasst.Minimierte Portlets können jederzeit wiederhergestellt werden.

6. Scannen von verwalteten Computern

Es gibt drei Möglichkeiten, Computer zu scannen, die durch Cloud Security for Endpoints geschützt sind:

- Der am Computer angemeldete Benutzer kann einen Scan über die Endpoint Security-Benutzeroberfläche starten.
- Sie können mithilfe der Richtlinie Scan-Aufgaben einplanen.
- Führen Sie eine Sofort-Scan-Aufgabe über die Konsole aus.

Um eine Scan-Aufgabe per Fernzugriff auf einem oder mehreren Computern auszuführen:

1. Öffnen Sie die Seite **Computer > Computer anzeigen**.Falls noch nicht geschehen, werden Sie zur Auswahl des Kundenunternehmens aufgefordert, das Sie verwalten möchten.
2. Klicken Sie in das **Anzeigen**-Menü oberhalb der Tabelle (auf der linken Seite) und wählen Sie **Verwaltete Computer**.
3. Wenn Sie Computer in Gruppen aufgeteilt haben, wählen Sie die gewünschte Gruppe im Bereich links aus.Um alle Ihre Computer anzuzeigen, klicken Sie mit der rechten Maustaste auf die Stammgruppe und wählen Sie **Alle Computer anzeigen**.
4. Markieren Sie die Kästchen für die Computer, die Sie scannen möchten.
5. Klicken Sie auf **Quick Tasks** und wählen Sie **Scan** aus dem Menü.
6. Wählen Sie die Scan-Art, die durchgeführt werden soll:
   - **Quick Scan** setzt auf In-the-Cloud-Scans, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.
   - Der **vollständige System-Scan** durchsucht den gesamten Computer nach allen Typen von Schad-Software, die ein Sicherheitsrisiko darstellen, so z.B. Viren, Spyware, Adware, Rootkits usw.
7. Klicken Sie auf **Scan anfordern**.Ein Bestätigungsfenster wird angezeigt.
8. Die Aufgabe können Sie unter **Computer > Aufgaben anzeigen** anzeigen und verwalten.

7. Hilfe erhalten

Für weitere Informationen oder Hilfe direkt von Bitdefender:

- Klicken Sie in der oberen rechten Bildschirmecke der Cloud Security Console auf **Hilfe und Support**.
- Besuchen Sie unser Online-Support-Center.

Um ein Support Ticket zu eröffnen, bitte füllen Sie dieses Web Formular aus.

A. Anforderungen

A.1. Systemanforderungen

Alle Bitdefender-Cloud-Sicherheitsdienste werden von der Cloud Security Console verwaltet.Da die Cloud Security Console gehostet wird, gibt es für die Verwaltung von Cloud Security for Endpoints keinerlei Hardware- oder Software-Anforderungen.Alles, was Sie brauchen, ist eine Internetverbindung.

Mindestanforderungen für Endpunkte

Betriebssysteme Arbeitsplatzrechner:

- Windows 8
- Windows 7
- Windows Vista mit Service Pack 1
- Windows XP mit Service Pack 3

Betriebssysteme Server:

- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Server 2008 R2
- Windows Server 2008
- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 SP1
- Windows Home Server

Eingebettete- und Tablet-Betriebssysteme*:

- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP Embedded mit Service Pack 2
- Windows XP Tablet PC Edition

*Bestimmte Betriebssystemmodule müssen für die Funktionalität von Cloud Security for Endpoints installiert werden.

Hardware-Anforderungen:

- Mit Intel® Pentium kompatibler Prozessor:

  Betriebssysteme Arbeitsplatzrechner:
  - 1 GHz oder schneller bei Microsoft Windows XP SP3, Windows XP SP2 64 Bit und Windows 7 Enterprise (32 und 64 Bit)
  - 2 GHz oder schneller bei Microsoft Windows Vista SP1 oder neuer (32 und 64 Bit), Microsoft Windows 7 (32 und 64 Bit), Microsoft Windows 7 SP1 (32 und 64 Bit), Windows 8
  - 800 MHZ oder schneller bei Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded mit Service Pack 2, Microsoft Windows XP Tablet PC Edition

  Betriebssysteme Server:
  - Minimum: 2,4 GHz Single-Core-CPU
  - Empfohlen: 1,86 GHz oder schnellere Intel Xeon Multi-Core-CPU
- Arbeitsspeicher:
  - Mindestens: 512 MB
  - Empfohlen: 1 GB
- Speicherplatz: 1,5 GB freier Speicherplatz auf der Festplatte

Internetzugang: Internet Explorer 8+, Mozilla Firefox 4+, Google Chrome, Safari oder Opera zum Endpunkt-Browser-Schutz und für den Zugriff auf die Cloud Security Console

A.2. Anforderungen für Netzwerkerkennung

Um alle Computer (Server und Arbeitsplatzrechner) erfolgreich zu erkennen, die über die Cloud Security Console verwaltet werden sollen, ist Folgendes erforderlich:

- Die Computer müssen in einer Arbeitsgruppe oder Domäne zusammengefasst und über ein lokales IPv4-Netzwerk verbunden sein.Der Computersuchdienst funktioniert nicht über IPv6-Netzwerke.
- In jeder LAN-Gruppe (Arbeitsgruppe oder Domäne) müssen mehrere Computer den Computersuchdienst ausführen. Auch die primären Domänencontroller müssen den Dienst ausführen.
- NetBIOS über TCP/IP (NetBT) muss auf den Computern aktiviert sein.Die lokale Firewall muss NetBT-Verkehr zulassen.
- Die Freigabe von Dateien muss auf den Computern aktiviert sein.Die lokale Firewall muss die Freigabe von Dateien zulassen.
- Eine Windows-Internet-Name-Service-Infrastruktur (WINS) muss eingerichtet und funktionsfähig sein.

- Für Windows Vista und höher muss die Netzwerkerkennung aktiviert werden (**Systemsteuerung > Netzwerk- und Freigabecenter > Erweiterte Freigabeeinstellungen ändern**).

  Um diese Funktion aktivieren zu können, müssen zunächst die folgenden Dienste gestartet werden:
  - DNS-Client
  - Funktionssuche-Ressourcenveröffentlichung
  - SSDP-Suche
  - UPnP-Gerätehost
- In Umgebungen mit mehreren Domänen empfiehlt es sich, Vertrauensstellungen zwischen den Domänen einzurichten, damit die Computer auch auf Suchlisten aus anderen Domänen zugreifen können.

Computer, über die Endpoint Security den Computersuchdienst abfragt, müssen in der Lage sein, NetBIOS-Namen aufzulösen.

Beachten Sie

Der Mechanismus zur Netzwerkerkennung funktioniert auf allen unterstützten Betriebssystemen, einschließlich der Windows-Embedded-Versionen, vorausgesetzt, dass alle Anforderungen erfüllt werden.